A construction for Hadamard arrays

Joan Cooper and Jennifer Wallis

We give a construction for Hadamard arrays and exhibit the arrays of orders \(4t\), \(t \in \{1, 3, 5, 7, \ldots, 19\}\). This gives seventeen new Hadamard matrices of order less than 4000.

An Hadamard matrix \(H\) of order \(h\) has every element \(+1\) or \(-1\) and satisfies \(HH^T = hI_h\), where \(I\) is the identity matrix of order \(h\). \(h\) is necessarily 1, 2, or congruent to zero modulo 4.

The Hadamard product, \(\ast\), of two matrices \(A = (a_{i,j})\), and \(B = (b_{i,j})\) which are the same size is given by

\[A \ast B = (a_{i,j}b_{i,j}).\]

We define an Hadamard array of order \(4n\), based on the indeterminates \(A, B, C\) and \(D\), to be a \(4n \times 4n\) array with entries chosen from \(A, -A, B, -B, C, -C, D\) and \(-D\) in such a way that:

(i) in any row there are \(n\) entries equal to \(A\) or \(-A\), \(n\) entries \(\pm B\), \(n\) entries \(\pm C\) and \(n\) entries \(\pm D\); and similarly for columns;

(ii) the rows are formally orthogonal, in the sense that if \(A, B, C\) and \(D\) are realized as any elements of any commutative ring then the rows of the array are pairwise orthogonal; and similarly for columns.

The Hadamard array of order 4 is

Received 17 May 1972.
\[
\begin{bmatrix}
A & B & C & D \\
-B & A & -D & C \\
-C & D & A & -B \\
-D & -C & B & A
\end{bmatrix}
\]

and is due to Williamson [10].

Suppose \( V \) is a finite abelian group with \( v \) elements, written in additive notation. A difference set \( D \) with parameters \((v, k, \lambda)\) is a subset of \( V \) with \( k \) elements and such that in the totality of all the possible differences of elements from \( D \) each non-zero element of \( V \) occurs \( \lambda \) times.

If \( V \) is the set of integers modulo \( v \) then \( D \) is called a cyclic difference set: these are extensively discussed in Baumert [11].

A circulant matrix \( B = [b_{i,j}] \) of order \( v \) satisfies \( b_{i,j} = b_{i,j-i+1} \) (\( j-i+1 \) reduced modulo \( v \)), while \( B \) is back-circulant if its elements satisfy \( b_{i,j} = b_{i,j+j-1} \) (\( i+j-1 \) reduced modulo \( v \)).

Throughout the remainder of this paper I will always mean the identity matrix and \( J \) the matrix with every element \( +1 \), where the order, unless specifically stated, is determined by the context. The Kronecker product of two matrices will be denoted by \( \times \).

Let \( S_1, S_2, \ldots, S_n \) be subsets of a finite abelian group \( V \), \(|V| = v\), containing \( k_1, k_2, \ldots, k_n \) elements respectively. Write \( T_\ell \) for the totality of all differences between elements of \( S_\ell \) (with repetitions), and \( T \) for the totality of elements of all the \( T_\ell \). If \( T \) contains each non-zero element of \( V \) a fixed number of times, \( \lambda \) say, then the sets \( S_1, S_2, \ldots, S_n \) will be called \( n = \{v; k_1, k_2, \ldots, k_n; \lambda\} \) supplementary difference sets.

The parameters of \( n = \{v; k_1, k_2, \ldots, k_n; \lambda\} \) supplementary difference sets satisfy

\[
(1) \quad \lambda(v-1) = \sum_{\ell=1}^{n} k_\ell (k_\ell - 1).
\]
If \( k_1 = k_2 = \ldots = k_n = k \) we will write \( \nu = (\nu; k; \lambda) \) to denote the supplementary difference sets and (1) becomes
\[
\lambda(\nu-1) = nk(k-1).
\]


The incidence matrix \( A = (a_{ij}) \) of a subset \( X \) of an abelian group \( G \) of order \( \nu \), with elements \( g_1, g_2, g_3, \ldots, g_\nu \), is found by choosing
\[
a_{ij} = \begin{cases} 1 & \text{if } g_j - g_i \in X, \\ 0 & \text{otherwise.} \end{cases}
\]

If \( A_1, A_2, \ldots, A_n \) are the incidence matrices of \( \nu = (\nu; k_1, k_2, \ldots, k_n; \lambda) \) supplementary difference sets then
\[
\sum_{i=1}^{n} A_i A_i^T = \left( k - \lambda \right) I + \lambda J,
\]
and the \((1, -1)\) matrices \( B_i = 2A_i - J \) satisfy
\[
\sum_{i=1}^{n} B_i B_i^T = \left( k - \lambda \right) I + \left( k - 4\lambda \right) J.
\]

We define the matrix \( R = (r_{ij}) \) of order \( \nu \) on \( G \) by
\[
r_{ij} = \begin{cases} 1 & \text{if } g_i + g_j = 0, \\ 0 & \text{otherwise.} \end{cases}
\]

For example, if \( G \) is the integers modulo \( n \) with the usual ordering,
\[
r_{i, n-i} = 1, \quad r_{ij} = 0 \text{ otherwise.}
\]

The construction

**Theorem 1.** Suppose there exist four \((0, 1, -1)\) matrices \( X_1, X_2, X_3, X_4 \) of order \( n \) which satisfy

(i) \( X_i \ast X_j = 0 \), \( i \neq j \), \( i, j = 1, 2, 3, 4 \),
(ii) \[ \sum_{t=1}^{h} X_tX_t^T = nI_n. \]

Suppose \( x_t \) is the number of positive elements in each row and column of \( X_t \) and \( y_t \) is the number of negative elements in each row and column of \( X_t \). Then

(a) \[ \sum_{t=1}^{h} (x_t y_t) = n, \]

(b) \[ \sum_{t=1}^{h} (x_t - y_t)^2 = n. \]

Proof. (a) follows immediately from (ii). To prove (b) we consider the four \((1,-1)\) matrices

\[
Y_1 = -X_1 + X_2 + X_3 + X_4, \\
Y_2 = X_1 - X_2 + X_3 + X_4, \\
Y_3 = X_1 + X_2 - X_3 + X_4, \\
Y_4 = X_1 + X_2 + X_3 - X_4.
\]

From [7] we know that \( h = \{n; k_1, k_2, k_3, k_4; \sum_{t=1}^{h} k_t - n\} \)

supplementary difference sets may be used to form an Hadamard matrix of order \(hn\). Now

\[ \sum_{t=1}^{h} Y_tY_t^T = hnI_n, \]

so \( E_t = \frac{1}{2}(Y_tY_t^T) \), \( t = 1, 2, 3, 4 \) are the incidence matrices (or permutations of them) of

\[
h = \{n; y_1y_2+\omega_3y_3+\omega_4y_4, y_1\omega_2+\omega_3y_3+\omega_4y_4, y_1y_2+\omega_3y_3+\omega_4y_4; 2 \sum_{t=1}^{h} x_t \}
\]

supplementary difference sets. Using (1) we have

\[ 2 \sum_{t=1}^{h} x_t(n-1) = \frac{h}{2} \left( x_1+x_2+x_3+x_4-y_t-y_t\right) \left( x_1+x_2+x_3+x_4+y_t-y_t\right), \]
or writing \( x_1 + x_2 + x_3 + x_4 = \omega \), \( t = y_1 + y_2 + y_3 + y_4 \), \( n = \omega + t \),

\[
2\omega(n-1) = \sum_{t=1}^{4} (x_t y_{t} \omega y_{t} - x_{t} \omega - 1)
= \omega y^2 + 2\omega \sum_{t=1}^{4} (y_{t} - x_{t}) + \sum_{t=1}^{4} (y_{t} - x_{t})^2 - \sum_{t=1}^{4} (y_{t} - x_{t})^2 - \omega y
= \omega y^2 + 2\omega(t-\omega) + \sum_{t=1}^{4} (y_{t} - x_{t})^2 - (t-\omega) - \omega y.
\]

So

\[
\sum_{t=1}^{4} (y_{t} - x_{t})^2 = n,
\]

as required.

**THEOREM 2.** Suppose there exist four \((0, 1, -1)\) circulant matrices \(X_1, X_2, X_3, X_4\) of order \(n\) satisfying the conditions of the above theorem. Then there exists a Hadamard array of order \(\sqrt{n}\).

**Proof.** Consider the following matrices, where \(A, B, C, D\) are indeterminates which commute in pairs

\[
Y_1 = X_1 \times A + X_2 \times B + X_3 \times C + X_4 \times D,
Y_2 = X_1 \times -B + X_2 \times A + X_3 \times D + X_4 \times -C,
Y_3 = X_1 \times -C + X_2 \times -D + X_3 \times A + X_4 \times B,
Y_4 = X_1 \times -D + X_2 \times C + X_3 \times -B + X_4 \times -A,
\]

and

\[
H = \begin{bmatrix}
Y_1 & Y_{2R} & Y_{3R} & Y_{4R} \\
-Y_{2R} & Y_1 & -Y_{3R} & Y_{4R} \\
-Y_{3R} & Y_{2R} & Y_1 & -Y_{2R} \\
-Y_{4R} & Y_{3R} & Y_{2R} & Y_1 \\
\end{bmatrix},
\]

where \(R\) is the Goethals-Seidel matrix (see \([3, 6]\)).

Now clearly \(H\) is of order \(\sqrt{n}\). Since each indeterminate is
associated with \( X_1, X_2, X_3 \) and \( X_4 \) in each row and column, and (a) of Theorem 1 holds, each indeterminate occurs exactly \( n \) times in each row and column. It may be verified that

\[
HH^T = I_n \times \sum_{i=1}^{h} Y_i X_i^T.
\]

It remains to show that

\[
\sum_{i=1}^{h} Y_i X_i^T = nI_n \times (AA^T + BB^T + CC^T + DD^T);
\]

but this is clearly true since \( \sum_{i=1}^{h} X_i X_i^T = nI_n \).

There is an equivalent enunciation for both Theorems 2 and 3 when \( X_1, X_2, X_3, X_4 \) are matrices defined on subsets of abelian groups.

**THEOREM 3.** Suppose there exist four circulant \((0, 1, -1)\) matrices \( X_1, X_2, X_3, X_4 \) of order \( n \) which satisfy

(i) \( X_i * X_j = 0 \), \( i \neq j \), \( i, j = 1, 2, 3, 4 \),

(ii) \( \sum_{i=1}^{h} X_i X_i^T = nI_n \).

Further suppose there exist four \((1, -1)\) matrices \( A, B, C, D \) of order \( m \) which pairwise satisfy \( MN^T = NM^T \) and for which

\[
AA^T + BB^T + CC^T + DD^T = hmI_m.
\]

Then there exists a Hadamard matrix of order \( bm \).

Proof. This follows by replacing the indeterminates \( A, B, C, D \) of the previous theorem by the matrices \( A, B, C, D \).

**COROLLARY 4.** There exists an Hadamard array of order \( 4t \) for \( t \in \{x : x \text{ is an odd integer, } 1 \leq t \leq 19\} \).

Proof. The matrices \( X_1, X_2, X_3, X_4 \) for \( t = 7, 9, 11 \) may be found in [6]. These matrices were found by Welch for \( t = 5 \), (unpublished result) but we give it here for completeness.
In each case we give a set which may be used to determine the first row of \( X_1, X_2, X_3, X_4 \). This is possible because the \( X_i \) are circulant. If \( \pm i \) is in the set for \( X_j \), then the \( i \)-th element of the first row of \( X_j \) is \( \pm 1 \), all the other elements are zero. Use the sets from the following table:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( X_1, X_2, X_3, X_4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>( 1^2+1^2+1^2+0^2 )</td>
</tr>
<tr>
<td>5</td>
<td>( 2^2+1^2+0^2+0^2 )</td>
</tr>
<tr>
<td>7</td>
<td>( 2^2+1^2+1^2+1^2 )</td>
</tr>
<tr>
<td>9</td>
<td>( 2^2+2^2+1^2+0^2 )</td>
</tr>
<tr>
<td>11</td>
<td>( 3^2+0^2+0^2+0^2 )</td>
</tr>
<tr>
<td>13</td>
<td>( 3^2+1^2+2^2+0^2 )</td>
</tr>
<tr>
<td></td>
<td>( 2^2+2^2+0^2+2^2 )</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>( 2^2+2^2+2^2+1^2 )</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td>15</td>
<td>( 3^2+2^2+1^2+1^2 )</td>
</tr>
<tr>
<td>17</td>
<td>( 4^2+1^2+0^2+0^2 )</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td>19</td>
<td>( 3^2+3^2+1^2+0^2 )</td>
</tr>
</tbody>
</table>

The matrices \( X_1, X_2, X_3, X_4 \) for \( n = 13 = 3^2 + 2^2 + 0^2 + 0^2 \) were found by listing the multiplicative cyclic group of order 12 generated by 2 to form the subgroup \( G_0 = \{2^{bj} : j = 0, 1, 2\} \) of order 3 and its
cosets \( C_i = \{2^{8j+i} : j = 0, 1, 2\}, \ i = 1, 2, 3 \). Then the first rows of \( X_1, X_2, X_3, X_4 \) may be obtained by using the sets
\[
C_0 \cup \{-C_1\}, \ C_3 \cup \{-13\}, \ C_2, \ \emptyset
\]
or
\[
C_2 \cup \{-C_3\}, \ C_1 \cup \{-13\}, \ C_0, \ \emptyset
\]
where \( -C_i = \{-i : i \in C_i\} \), and the \( X_j \) are formed as described in the proof of Corollary 4.

For \( n = 19 = 3^2 + 3^2 + 1^2 + 1^2 \) the multiplicative cyclic group of order 18 generated by 2 was used to form the subgroup
\[ C_0 = \{2^{6j} : j = 0, 1, 2\} \] of order 3 and its cosets
\[ C_i = \{2^{6j+i} : j = 0, 1, 2\}, \ i = 1, \ldots, 5. \]
Then \( X_1, X_2, X_3, X_4 \) were found, as above, by using the sets
\[ C_1, C_3, C_2 \cup \{-C_1\}, \{0\} \cup C_4 \cup \{-C_2\}. \]

Matrices \( A, B, C \) and \( D \) satisfying the conditions of Theorem 3 have previously been used to construct Hadamard matrices of orders \( 4m \) \([10]\), \( 12m \) \([12]\), \( 20m \) (unpublished result of Welch, communicated to the authors by Baumert), \( 28m \), \( 36m \), \( 44m \) \([6]\). They are known to exist when \( m \) is a member of the set
\[ M = \{3, 5, 7, \ldots, 29, 37, 43\}, \]
\([4]\), and when \( 2m - 1 \) is a prime power congruent to 1 modulo 4 \([5, 9]\).

**COROLLARY 5.** There exist Hadamard matrices of orders \( 52m \), \( 60m \), \( 68m \), \( 76m \) whenever \( m \in M \).

**COROLLARY 6.** There exist Hadamard matrices of orders \( 26(q+1) \), \( 30(q+1) \), \( 34(q+1) \), \( 38(q+1) \) whenever \( q \) is a prime power congruent to 1 modulo 4.

This gives the following new Hadamard matrices of order \( < 40000: \)
\[
988, 1196, 1444, 1508, 1564, 1612, 1900, 1972, 2108, 2356, 2516, 2788, 2924, 3116, 3128, 3172, 3876.
\]
References


Department of Mathematics, University of Newcastle, New South Wales.